Contenido

Introducción

Este documento describe el proceso para resolver problemas el Integración de telefonía de computadora (CTI) seguro para Cisco unificó la integración de la comunicación (UC) con IBM Sametime.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento del administrador de las Comunicaciones unificadas de Cisco.

Componentes Utilizados

La información en este documento se basa en Cisco unificó la versión 8.x del administrador de llamada.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Troubleshooting

1. Asegúrese que el token de seguridad haya estado instalado en el Cisco Call Manager.
   - Van los **parámetros al > Security (Seguridad) de la página de administración > del System (Sistema) > Enterprise Parameters (Parámetros Enterprise) del administrador de llamada**.
   - Si el modo seguro del cluster es el "0", éste indica que Certificate Trust List (Lista de confianza del certificado) no configuran ni que están instalado al cliente (CTL)

en el modo seguro.
    - El modo seguro del cluster es el "1" cuando ha estado instalado.
2. Asegúrese que el usuario haya habilitado las funciones de seguridad.
    - Va a la **página de administración del administrador de llamada > User Management (Administración de usuario) > el usuario final - > información de los permisos**.
3. Asegúrese que la “conexión segura estándar CTI” esté agregada a los permisos del grupo.
4. Verifique al cliente que los archivos de la función de proxy del Certificate Authority (CAPF) se crean y que se nombran correctamente.
    - Va a la **página de administración del administrador de llamada > User Management (Administración de usuario) > el perfil del CAPF del usuario final**.
    - Asegúrese que los archivos del CAPF para el usuario estén creados.
    - El formato para el caso ID del archivo del CAPF debe ser ><num> de la identificación del usuario del administrador del <Call donde está un número entero el <num> a partir de la "0" hasta el "4".
5. Verifique al cliente y servidor que los archivos de certificado se han descargado con éxito.
    - Estos archivos se localizan en:
      Windows XP: <username> \ Configuraciones locales \ datos de aplicación \ Cisco \ SametimePhone \ Certificados \ (de C:\Documents and Settings\ Windows XP)Windows 7: De C:\Users\ <username> \ AppData \ Local \ Cisco \ SametimePhone \ Certificados \Directory Name (Nombre de directorio) comienza con el <username><server> y debe contener:
      Por lo menos un archivo del servidorUn archivo clienteUn archivo CTLEjemplos de archivo para el usuario “johndoe”:
      CTLFile.tlv.sgnJtapiServerKeySote-johndoe-johndoe0JtapiClientKeyStore-johndoe-johndoe0
6. Asegúrese de que estos campos estén configurados correctamente en la sección segura de la conexión CTI de la utilidad de configuración:
    - “Se marca el indicador de la conexión segura del uso”
    - Servidor TFTP (generalmente el servidor de administración de la llamada)
    - Puerto TFTP (valor por defecto 69)
    - Servidor del CAPF (generalmente el servidor de administración de la llamada)
    - Puerto del CAPF (valor por defecto 3804)
    - Vaya a las **preferencias de Sametime > a Cisco > al control del teléfono**, y asegúrese que el campo de los “servidores” no es editable. No se permite cambiar a los servidores de seguridad en el tiempo de ejecución.

El administrador puede fijar este campo como solo lectura, pero si es editable el CTI seguro no se habilita.

Información Relacionada

- Integración de Cisco UC para IBM Sametime
- Soporte Técnico y Documentación - Cisco Systems